LA-UR-13-24366
Approved for public release; distribution is unlimited.

Title: NLIT DOE Control System Security BOF

Author(s): Frost, Sandra L.

Intended for: National Laboratories Information Technology Summit 2013,
2013-05-13/2013-05-16 (Santa Fe, New Mexico, United States)

Issued: 2013-06-14

NLIT DOE Control System Security BOF

Sandy Frost/LANL

Agenda

- DOE Control System Security monthly web meetings

Monthly Web Meetings

Presentation	Speaker
Symantec Critical System Protection	Constanza/LANL
Asset Management – Monitoring Access	Roberts/LANL
Control System Penetration Testing	Petruzzi/HSS Auditor
Wireless Networked ARMs and CAMS	Gregory/SRS
Overview of the EMS System and SCADA Related Initiatives, WAPA Rocky Mountain Region	Aust/WAPA
Cyber Security in the Pacific Northwest Smart Grid Demonstration	Akyol/Battelle
Aurora – Power at Risk	Lopez/LANL
Firmware Management	Frost/LANL
SANS N. American ICS & SCADA Summit Summary	Jones/INL, Harkleroad/ORNL, Justice/LANL, Frost/LANL
Sophia Tool	Tchilinguirian/PPPL
Control System Security Training	Parks/SNL, Frost/LANL
Supply Chain Risk Management (next month)	Minihan/KCP, Wegener/KCP, Frost/LANL

Agenda

- DOE Control System Security monthly web meetings

- Discussion on “Bringing Legacy Control System Networks into the Cyber Fold”, Karl Black/INL

Agenda

- DOE Control System Security monthly web meetings
- Discussion on “Bringing Legacy Control System Networks into the Cyber Fold”, Karl Black/INL
- Improving Critical Infrastructure Cyber Security Workshop Video

Backup Slides

Improving Critical Infrastructure Cybersecurity Workshop Video Available On Demand

From NIST *Tech Beat*: April 17, 2013

Contact: Evelyn Brown
301-975-5661

The video of the April 3, 2013, Cybersecurity Framework Workshop convened by the National Institute for Standards and Technology (NIST) is now available for streaming on demand. This meeting, held at the Department of Commerce in Washington, D.C., brought together experts in cybersecurity and critical infrastructure to discuss what issues stakeholders believe should be covered in the framework.

In a February 2013 Executive Order "Improving Critical infrastructure Cybersecurity," the President called for NIST to work with industry this year to develop a voluntary framework for reducing cyber risks to critical infrastructure. Critical infrastructure is defined as systems critical to the country's security, including economic and public health safety. This framework will be designed to help infrastructure owners and operators to manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties.

The "Cybersecurity Framework Workshop" video includes keynotes by Rebecca Blank, deputy secretary, Department of Commerce; Michael Daniel, special assistant to the President and Cybersecurity Coordinator; Jane Holl Lute, deputy secretary, Department of Homeland Security; and Patrick Gallagher, Undersecretary of Commerce for Standards and Technology and director of NIST.

The moderated discussions include "Industry Leaders Perspectives," "Current Threat Environment for Critical Infrastructure – an Industry Perspective," "Developing the Cybersecurity Framework: Industry Roundtable," "Critical Infrastructure Partnership and the Cybersecurity Framework," and "The Path Forward: Panel Discussion."

During the April 3, 2013 Cybersecurity Framework Workshop, Commerce Deputy Secretary Rebecca Blank calls for critical infrastructure owners and operators to work closely with NIST to develop a strong, voluntary cybersecurity framework that will keep the country safe.

RFI - Framework for Reducing Cyber Risks to Critical Infrastructure

Comments Received in Response To:

[Federal Register Notice Developing a Framework To Improve Critical Infrastructure Cybersecurity]

Last updated: April 29, 2013

Date	Received From	Date	Received From
February 13, 2013	MaCT Part 1	February 26, 2013	MaCT Part 2
February 26, 2013	MaCT Part 3	February 26, 2013	Piltz
February 26, 2013	TAG Universal Machine Part 1	February 26, 2013	TAG Universal Machine Part 2
February 27, 2013	DOD JS J7 Part 1	February 27, 2013	DOD JS J7 Part 2
...			
March 25, 2013	Argonne National Laboratory	March 26, 2013	Tri-County Electric Cooperative, Inc., Part 1
...			
April 8, 2013	DoE	April 8, 2013	FireEye
...			
April 11, 2013	System 1	April 11, 2013	Idaho National Laboratory

http://csrc.nist.gov/cyberframework/rfi_comments.html

Executive Order – Improving Critical Infrastructure Cybersecurity

Sec	Title	
1	Policy	It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.
2	Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
3	Policy Coordination	
4	Cybersecurity Information Sharing	Increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.
5	Privacy and Civil Liberties Protections	Ensure that privacy and civil liberties protections are incorporated into such activities.
6	Consultative Process	Establish process for improvements to framework.
7	Baseline Framework to Reduce Cyber Risk to Critical Infrastructure	NIST leads development of framework.
8	Voluntary Critical Infrastructure Cybersecurity Program	Establish voluntary program to support the adoption of the framework by owners & operators.
9	Identification of Critical Infrastructure At Greatest Risk (150 days)	Use risk-based approach to identify critical infrastructure where a cybersecurity incident cold reasonably result in catastrophic effects on public health or safety, economic security or national security.
10	Adoption of Framework	Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB and the Nat. Security staff.

http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

What is “Critical Infrastructure”?

EX. ORD. NO. 13010. CRITICAL INFRASTRUCTURE PROTECTION

Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property (“physical threats”), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures (“cyber threats”). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.

http://www.gpo.gov/fdsys/pkg/USCODE-2011-title42/html/USCODE-2011-title42-chap68-subchapIV-B-sec5195.htm